PRIVACY IMPACT ASSESSMENT

1. DoD Component: Defense Logistics Agency (DLA).

2. Name of IT System: DLA iComplaints tool.

3. Budget System Identification Number: N/A.

4. System Identification Number: N/A.

5. IT Investment Unique Identifier: N/A.

6. Privacy System of Records Notice Identifier: U.S. Equal Employment Opportunity Commission (EEOC)/Govt-1, Equal Employment Opportunity (EEO) in the Federal Government Complaint and Appeal Records.

7. OMB Information Collection Number and Expiration Date: Recordkeeping under Title VII and the ADA, OMB Control No. 3046-0040, expires November 30, 2006.

8. Authority: 42 U.S.C. 2000e-16(b) and (c); 29 U.S.C. 204(f) and 206(d); 29 U.S.C. 633(a); 29 U.S.C. 791; Reorg. Plan No. 1 of 1978, 43 FR 19607 (May 9, 1978); E.O. 12106, 44 FR 1053 (Jan. 3, 1979).

9. Brief Summary: MicroPact Engineering's iComplaints database tool will allow DLA to electronically manage EEO complaints agency-wide, specifically track and report on field EEO complaints. It will provide congressionally mandated reports with greater accuracy and reduced effort (e.g. the Annual Equal Employment Opportunity Statistical Report of Discrimination Complaints [the EEOC 462 Report]). The iComplaints software will also allow DLA to comply with the new reporting requirements of the Notification and Federal Employee Anti-Discrimination and Retaliation Act of 2001 (No FEAR) signed into law in May 2002.

IComplaints is a web-based browser. It is a tool that captures events and case details in the Federal EEO complaints process from the pre-complaint stage through the appeal and civil action stages IAW Title 29 of the U.S. Code of Federal Regulations (CFR), Part 1614. Records will be used for the purposes of case tracking, case management and as source information for EEOC statistical reporting requirements only. Records will be used to generate statistical reports to evaluate/analyze the status, trends and effectiveness of the EEO complaint process in DLA. Reports generated will not contain personally identifiable information.

IComplaints includes a set of business rules ensuring compliance with 29 CFR 1614, EEOC Management Directive (MD) 110, and EEOC reporting requirements.

IComplaints is designed to provide these capabilities in an environment offering maximum ease of use and making minimal maintenance demands on the client.

10. Identifiable Information to be Collected and Nature/ Source: The database relies on these personal identifiers: Individual's name, home address, home telephone number, work telephone number, and information about the alleged discrimination claim (basis[es], issue[s] and requested relief). An intake form entitled "EEO Pre-complaint in the Federal Government Information," and DLA Form 1808, entitled "Formal Complaint of Discrimination in the Federal Government Information," are used to collect the information directly from the subject individual.

11. Method of Information Collection: Paper and electronic forms.

12. Purpose of collection: To provide the necessary information and documentation required to counsel individuals who alleged they have been discriminated against; to conduct formal inquiries and investigations; and to adjudicate complaints of employment discrimination brought by applicants and current and former Federal employees IAW applicable statutes and regulations.

13. Data Uses: Data is used as a management tool to monitor/evaluate the status of the DLA complaint process and to counsel, investigate/adjudicate DLA complaints of employment discrimination. Statistical data is used to meet reporting requirements of the EEOC regarding the status of the DLA EEO complaint processing program. User permission of the data collected depends on assigned roles in the complaint process defined in 29 CFR Part 1614. Such roles and responsibilities are based in a secure environment. Reports produced using the data contain no personally identifiable information.

14. Does system create new data about individuals through aggregation? N/A.

15. Internal and External Data Sharing:

Internal to DLA: Data may be viewed by or shared with employees assigned to the DLA EEO offices such as EEO Managers, EEO Specialists, EEO Assistants, Agency attorneys, and EEO Investigators for the purposes of performing the agency's complaint processing functions under 29 CFR Part 1614.

External to DLA: Information collected may be shared through system generated reports with EEOC Administrative judges, Federal judges, attorneys, and others involved with an EEO case. Complaint information is shared with Complainants' attorney as appropriate. Case files are not stored in this IT tool. With a written request of the complainant, information from this database may be shared with congressional offices or attorneys retained by the complainant. Data from this tool will be shared with contracted counselors, employers of contract investigators and witnesses, as appropriate, to carry out the agency's complaint processing responsibilities under 29 CFR Part 1614.

16. Opportunities to object to the collection or to consent to the specific uses and how consent is granted: All personal data collected is voluntarily given by the complainant. The pre-complaint and formal complaint forms that collect personal data that is captured in iComplaints contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data or participating in the program. The Statement advises that participation is voluntary; however, failure to provide the requested information may inhibit the processing of the complaint.

17. Information provided the individual at collection, the format, and the means of delivery:

- A Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), is provided at the beginning of each stage of the EEO administrative complaint process when personal data is collected; pre-complaint and formal complaint stages. The Statement provides the following: authorities; collection purpose; external uses; the voluntary nature of the program and the fact that no consequences accrue for those who choose not to participate; the name and number of the Privacy Act system notice governing the collection, and an electronic link to the system notice. The Statement is included on paper and electronic collection forms.

- DLA Fair Information Principles, which govern all Privacy Act data collections, are published on the HQ DLA Home page. While not provided at the collection point, the Principles are contained in DLA Privacy Act training module "Privacy Act 101" – mandatory training for all DLA employees, military members, and contractors. The DLA workforce is required to be aware of the Principles to fulfill their duties in handling third party personal data and in learning their Privacy Act rights.

18. Data Controls:

Administrative: Users, including individuals responsible for system maintenance, receive initial and periodic refresher Privacy Act and Information Assurance training. Users are warned through log-on procedures of the conditions associated with access and the consequences of improper activities. Users are required to accept those conditions/consequences before logon completes. Users are trained to lock their workstations when leaving them unattended, to shut down computers when leaving at the end of the duty shift, and to be alert to third parties entering the workspace. Data is periodically backed up and stored in a secure facility.

Physical: The data resides on a computer system that is not connected to the World Wide Web. Central Processing Units are located in a secure computer facility physically controlled with either a badge/card swipe or read required for entry. Within the secure facility, central processing units are kept in locked or controlled access areas. Where possible, office layout is designed to keep computer terminals protected from the view of room visitors. Electronic records are backed up periodically. Areas housing central processing units, servers, and work stations are configured with a

fire suppression system. Should the system fail, the lost data could be constructed from the back-up records, paper files, and input sources.

Technical: The electronic records are deployed on accredited systems with access restricted by the use of login, password. The web-based files are encrypted in accordance with approved information assurance protocols. It uses built-in virus detection software with a notification system in place to alert administrators to new viruses and software-resistant viruses. Computer terminals are password controlled with system-generated forced password change protocols. All passwords are tested for strength at the time of selection. Computer screens automatically lock after a preset period of inactivity with re-entry controlled by password. Systems manually locked by the user also require password for reentry. Shutdown compliance is periodically checked. Workstations connecting to the system have real time virus/worm detection software installed.

19. Privacy Act Interface: The data and information maintained by iComplaints is covered by an existing government-wide Privacy Act system of records notice, EEOC/GOVT-1, entitled "Equal Employment Opportunity in the Federal Government Complaint and Appeal Records".

20. Potential threats in collecting, using, and sharing the information; dangers in providing notices or opportunities to object/consent or to providing notices to the individual; risks posed by the adopted security measures:

Threats: Data sharing occurs only among individuals authorized access to the system as stated in the governing Privacy Act system notice. All system users are made aware of restrictions on secondary uses of the data by initial and refresher Privacy Act and Information Assurance training.

Dangers: There are no dangers in providing notice of the collection or allowing an individual to object/consent. Therefore, individuals are given this opportunity at times of notice publication and data collection. Afterwards, individuals may raise objections if new threats are perceived.

Risks: The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards described in this document. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

21. Classification and Publication of Privacy Impact Assessment:

Classification: Unclassified.

Publication: This document will be published either in full or in summary form on the DLA public website, http://www.dla.mil/public_info/efoia/privacy.asp .

Data Owner: [redacted] (Signature) 3/20/06 (Date)

Name: Famia Magana
Title: Director, DLA Equal Employment Opportunity Office
Work Phone Number: [redacted]
Email: [redacted]

Information Assurance Officer: [redacted] (Signature) April 18, 2006 (Date)

Name: [redacted]
Title: Information Assurance Manager
Work Phone Number: [redacted]
Email: [redacted]

Privacy Officer: [redacted] (Signature) 20 Mar 06 (Date)

Name: Susan Salus
Title: DLA Privacy Act Officer
Work Phone Number: [redacted]
Email: [redacted]

DLA Privacy Technology Advisor: [redacted] (Signature) 21 Mar 06 (Date)

Name: Lew Oleinick
Title: DLA Privacy Technology Advisor
Work Phone Number: [redacted]
Email: [redacted]

Reviewing Official: [redacted] (Signature) 1 May 2006 (Date)

Name: Mae De Vincentis
Title: DLA Chief Information Officer
Work Phone Number: [redacted]
Email: [redacted]